ANALISA SERANGAN DDOS PADA SERVER UBUNTU ANG BEROPERASI DALAM WIRELESS LOCAL AREA NETWORK

Faris Muhamad[1], Agus Virgono[2], Burhanuddin Dirgantara[3]

[1]Teknik Telekomunikasi, Fakultas Teknik Elektro, Universitas Telkom

Abstrak

Saat ini serangan yang terjadi pada server sudah semakin mengkhawatirkan, sehingga diperlukan suatu penelitian yang meneliti serangan-serangan tersebut baik dari pola-pola serangannya maupun akibat yang ditimbulkan oleh serangan tersebut. Satu diantara serangan-serangan yang terjadi adalah (DDoS Distributed Denial of Service).

DDoS merupakan serangan untuk melumpuhkan layanan yang diberikan kepada user di mana user nanti tidak dapat mengakses server tersebut. Cara yang dilakukan oleh serangan DDoS adalah dengan mengirim paket sebanyak mungkin ke server dengan waktu yang sangat cepat. Agar paket yang dikirimkan dalam waktu singkat dalam jumlah yang besar maka diperlukan jumlah penyerang yang banyak pula.

Untuk tugas akhir ini, serangan terhadap server (web server) akan dilakukan pada server yang beroperasi pada WLAN karena pada WLAN penyerang akan berada dekat dengan target tetapi saat selesai melakukan serangan penyerang dapat melarikan diri tanpa harus repot membereskan peralatan yang dibawa untuk menyerang.

Serangan akan dilakukan dengan menggunakan jumlah user dan paket yang berbeda-beda dan didapatkan karakteristik dari serangan DDoS yaitu hanya menyerang bagian network dari target, menggunakan protokol ICMP untuk berkomunikasi dengan Zombie yang dimiliki, dan serangan dimulai dengan terjadinya kenaikan trafik yang cukup ektrim pada target dan setelah serangan berakhir trafik pada target akan menurun secara ekstrim pula.

Parameter-parameter yang mempengaruhi serangan DDoS yaitu interface yang digunakan untuk melakukan serangan, bit rate dari interface, serta jumlah penyerang yang melakukan serangan. Untuk mengetahui pelaku serangan dpat diketahui dari mac address yang tercapture dari pengirim paket. Lalu untuk mengantisipasi serangan DDoS dapat menggunakan iptables yang telah dimiliki oleh server dengan menambahkan aturan-aturan berdasarkan karakteristik dari serangan DDos yang telah diketahui untuk mencegah serangan itu kembali.

Kata Kunci : Sever, Zombie, Zabbix, Joomla, TFN, DDoS

Abstract

When this attack occurred on the server was getting worried, so required a study that examines these attacks both from the patterns of attack and the effects of the attack. One of the attacks that happened was (DDoS Distributed Denial of Service).

DDoS is an attack to disable the services provided to the user where the user will not be able to access the server. Way by DDoS attack is to send packets to the server as much as possible with a very fast time. In order for the package that was sent in a short time in large numbers will require a lot of attackers as well.

For this final task, the attack on the server (web server) will be done on the server that operates on WLAN WLAN because the attacker will be close to the target but when finished the attack the attacker can escape without the hassle of cleaning equipment was brought to attack.

The attack will be carried out by using the number of users and package different and acquired characteristics of DDoS attacks are only attacking the network from the target, using the ICMP protocol to communicate with Zombie owned, and the attack begins with the increase in traffic which is extremely on target and after the attack on the target end traffic will decrease too extreme.

The parameters that affect the DDoS attack is the interface that is used to conduct attacks, bit rate of the interface, and the number of attackers who carried out the attack. The attacker found by captured mac address of the sender packet. So in anticipation of DDoS attacks can use iptables already owned by the server by adding the rules based on the characteristics of DDos attacks which have been known to prevent the attack again.

Keywords : Sever, Zombie, Zabbix, Joomla, TFN, DDoS

BAB I

PENDAHULUAN

1.1 LATAR BELAKANG

Seiring perkembangan serangan terhadap *server* di dalam dunia sistem computer yang sudah semakin variatif, maka diperlukan suatu riset yang meneliti karakteristik dari suatu serangan yang dilakukan terhadap suatu *server* , akibat yang dihasilkan oleh serangan tersebut terhadap *server*, dan bagaimana suatu *server* dapat mengenali user mana yang berpotensi sebagai penyerang sehingga kemampuan keamanan yang dimiliki oleh *server* dapat meningkat.

Untuk tugas akhir ini, yang menjadi pokok pembicaraan adalah *DDoS* (Distributed Denial of Service) di mana serangan ini bertujuan untuk melakukan Downtime terhadap *server* agar tidak dapat diakses oleh user. Serangan ini umumnya membanjiri *server* dengan paket-paket dengan memanfaatkan kelemahan three way hanshaking pada TCP sehingga *server* tersebut menjadi sibuk. Agar paket yang dikirim bisa dalam jumlah yang besar, maka penyerang membutuhkan pasukan (*Zombie*) untuk membantu melakukan hal tersebut. Dan serangan ini lebih mudah saya implementasikan dibandingkan jenis serangan yang lain.

Lalu digunakan *server* Ubuntu karena memang saya lebih terbiasa menggunakan sistem operasi Ubuntu untuk *server* dan terdapat komunitas yang dapat membantu bila ada masalah dalam membuat *server*, serta terdapat *server repository* internal kampus sehingga memudahkan dalam mencari program-program yang ingin dicari.

Wireless LAN yang digunakan karena mudah dalam pembuatan jaringannya, mulai banyak digunakan utnuk membuat *hotspot* untuk *internet* pada tempat-tempat umum, dan akan memudahkan penyerang dalam melakukan serangan dan melarikan diri setelah melakukan serangan. Dan akan dilihat pula apakah mempengaruhi serangan yang akan dilakukan oleh penyerang.

1.2 TUJUAN

1. Mengetahui karakteristik serangan *DDoS* yang dilakukan terhadap suatu *server*.
2. Mendapatkan parameter-parameter yang mempengaruhi serangan *DDoS* terhadap suatu *server*.
3. Menemukan user yang berpotensi menyerang *server* tersebut.

1.3 PERUMUSAN MASALAH

Pada tugas akhir ini masalah yang akan dihadapi yaitu bagaimana serangan *DDoS* dapat terjadi, parameter apa saja yang mempengaruhi serangan *DDoS*, dan bagaimana mengetahui siapa yang berpotensi melakukan penyerangan tersebut.

1.4 METODOLOGI PENELITIAN

1. Studi literatur.
2. Simulasi.

1.5 BATASAN MASALAH

Beberapa hal yang dibatasi dalam tugas akhir ini sebagai berikut :

1. *Server* yang digunakan menggunakan *operating system* Ubuntu *Server*.
2. Dilakukan pada *Wireless* Local Area Network (WLAN).
3. Serangan yang dilakukan yaitu *DDoS* menggunakan program TFN.
4. *Server* memiliki *Zabbix* dan *Wireshark* untuk melihat aktivitas dari *server* tersebut.
5. Tidak membahas teknik *Hacking* .

1.6 Sistematika Penulisan

Sistematika penulisan tugas akhir ini adalah :

BAB I PENDAHULUAN

Bab ini berisi uraian singkat mengenai latar belakang permasalahan, perumusan masalah, maksud dan tujuan penelitian, batasan masalah, metode penelitian serta sistematika penulisan.

BAB II DASAR TEORI

Bab ini berupa uraian konsep dan teori dasar secara umum yang mendukung dalam pemecahan masalah, baik yang berhubungan dengan sistem maupun perangkat.

BAB III PERANCANGAN SISTEM

Pada Bab ini dibahas mengenai perancangan dan implementasi sistem untuk mengukur serngan *DDoS*.

BAB IV PENGUJIAN DAN ANALISA

Bab ini menguraikan pengujian dan analisa prinsip kerja sistem yang telah diimplementasikan. Pengujian dan analisa sistem akan mengacu pada waktu rata-rata pengiriman, jumlah user, dan kecepatan pengiriman paket berdasarkan jumlah paket.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi tentang kesimpulan dan saran terhadap hasil yang diperoleh dari penelitian yang telah dilakukan.

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Kesimpulan yang didapat dari tugas akhir ini adalah :

1. Karakteristik serangan DDoS yaitu :
   a) Serangan dimulai dengan trafik jaringan yang naik secara ekstrim dari kondisi semula.
   b) Menyerang dengan mengirimkan paket dalam jumlah yang banyak dan membutuhkan waktu yang singkat.
   c) Menggunakan protocol ICMP untuk berkomunikasi keapada *zombie* untuk memulai dan mengakhiri serangan.
   d) IP penyerang bersifat *random* tetapi MAC address bersifat *static*.

2. Parameter-parameter yang mempengaruhi serangan *DDoS* yaitu :

   a). *Interface* yang digunakan

   b). *Bit rate* dari *interface* yang digunakan

   c). Jumlah penyerang

3. Penyerang dapat diketahui dari MAC address yang didapatkan dari hasil *capture packet*, dan IP address penyerang diketahui dari tabel ARP yang dimiliki oleh server. Setelah itu serangan dapat dicegah menggunakan *iptables.*

4. Dengan menggunakan *fastethernet (wired)* waktu yang dibutuhkan untuk diterimanya paket oleh server lebih cepat hingga 5 kali dibandingkan dengan menggunakan *wireless* .

5. Dengan menggunkan bit rate 100 Mbps maka kecepatan diterimanya paket oleh server naik hingga 9 kali jika dibandingkan dengan mengggunakan 54 Mbps.

5.2 Saran untuk penelitian selanjutnya

1. Coba server menggunakan berbagai sistem operasi yang berbeda agar diketahui apakah sistem operasi mempengarui juga.
2. Jumlah penyerang diperbanyak.
3. Gunakan program *DDoS* yang berbeda seperti *trinoo, tear drop*, atau menggunakan *spybot.*